Evaluation of cyber security in agile manufacturing: Maturity of Technologies and Applications

Halldor Arnarson[1], Faraz Safarpour Kanafi[2], Tero Kaarlela[3], Ulrich Seldeslachts[4] and Roel Pieters[5]

***Abstract*— Utilizing Industry 4.0 technologies offers SMEs a possibility to increase productivity. Utilizing new technologies requires connectivity between production equipment, which raises Cyber Security (CS) issues that need to be addressed. In this work we analyse 18 demonstrators that are representative for different technologies and applications, and are of interest to the digitization of factories and agile production. CS analysis was performed by CS questionnaires to evaluate the current level of CS. As small and medium sized companies (SMEs), and researchers, may be unaware of CS issues, we provide general recommendations and measures to secure production systems from CS attacks.**

I. INTRODUCTION

In the past, industrial production systems were isolated and utilized networking protocols incompatible with IT-systems. Isolation from IT-systems provided protection against outside Cyber Security (CS) threats for production networks. However, during the last decades, demand for connectivity has driven industries to adopt common internet standards TCP/IP and Ethernet [1], [2]. Utilization of common internet standards enable trivial connectivity and data sharing between production equipment and the internet. As a downside, utilization of internet protocols require exposing industrial production systems to CS threats and attacks. Industrial systems set higher requirements for latency, speed and reliability, compared to IT-systems [3], thereby setting high demands for CS implementations.

Industry 4.0 technologies have proven potential to push industry towards growth [4]. Utilization of advanced technologies such as cloud computing, Internet of things (IoT), artificial intelligence, and big data are enabled by Industry 4.0. Exploitation of advanced technologies in smart factories require connectivity, exposing production machinery to CS risks, vulnerabilities and threats. Recent studies have identified CS threats as a risk to manufacturing and the digitalization of factories [5], [6]. CS attacks can lead to production shutdown, industrial espionage, information leaks and physical damages. CS is also a building block of physical safety as modern cyber-physical systems (CPS) enables intruders a possibility to cause physical damages and injuries. Thus, besides the technology itself, also physical processes, people, and even intellectual property [7] might be compromised by poor CS.

Different modes of operations for industrial and connected robots and systems start with controllers, following PLCs, ROS versions 1 and 2, IoT, and the Cloud. ROS version 1 was not designed with CS in mind, and CS is considered from ROS2 on [8], [9]. SMEs integrate the operation modes from ROS toward the newer features. The problem today is that reaching a sufficient level of CS can be too expensive for SMEs. Implementing high level CS requires investing into knowledge, devices and software products. The constant need for training of personnel, updating of devices and software tools, is too expensive for many SMEs. Therefore, SMEs may lag behind in the adoption of CS and measures taken to have a secure system. Fortunately, lately a variety of tools for the self evaluation of CS maturity levels are becoming available [10].

This paper presents a CS evaluation on selected agile manufacturing use case demonstrators of Horizon 2020 (H2020) project TRINITY[1]. Demonstrators present state-of-the-art solutions and are offered for European SMEs to adopt. CS evaluation is carried out with an evaluation tool created during the project. Results of the evaluation are the current CS knowledge level of each demonstrator and measures to take to improve the CS to a higher level. The contributions of this work are as follows:

1) Overview of the state-of-the-art in standards/initiatives towards CS in manufacturing
2) CS analysis of 18 demonstrators that offer technology and applications to make SMEs more agile in their production
3) Provide (general) recommendations for manufacturing companies and manufacturing SMEs in particular on practical steps to improve their CS

The paper is organized as follows. Section II presents a brief overview of current state of the art CS for production systems. Current standards, protocols and vulnerability assessments methods for CS are presented in Section III. The use case demonstrators and their CS analysis are presented in Section IV, and discussed in Section VI. The paper concludes in Section VII.

[1] Halldor Arnarson is with the Department of Industrial Engineering, UiT The Arctic University of Norway, Narvik Norway, halldor.arnarson@uit.no

[2] Faraz Safarpour Kanafi is with the Department of Computer Science and Computational Engineering, UiT The Arctic University of Norway, Narvik Norway, fka024@post.uit.no

[3] Tero Kaarlela is with Centria University of Applied Sciences, Vierimaantie 7, 84100 Ylivieska, Finland, tero.kaarlela@centria.fi

[4] Ulrich Seldeslachts is with LSEC Leaders In Security, Leuven, Belgium, ulrich@anakyn.be

[5] Roel Pieters is with Unit of Automation Technology and Mechanical Engineering, Tampere University, Finland, roel.pieters@tuni.fi

[1] https://trinityrobotics.eu

II. State of the art

The current state of CS in smart manufacturing systems is reviewed in [2], [11], presenting important reported attacks against smart manufacturing systems and available active and passive countermeasures with their limitations. A comprehensive overview of CS in robotics applications is presented in a recent review [12], covering different aspects, such as vulnerabilities, attacks, countermeasures, and recommendations. Interesting reviews of CS in other specific application areas have also been published. In particular, CS for industrial control systems [13], [14], digital manufacturing [15] and the Internet of Things [9] has been reviewed widely. An overview of robot hazards [16], security modelling of autonomous systems [17] and social robots [18] help in outlining CS for robotics.

Technical evolution has recently reshaped the horizon of CS. In the past, the focus of CS was to protect company networks from outside access. Restriction of networks were implemented by firewalls, malware protections and intrusion detection systems [19]. Today, connectivity of devices and networks have enabled possibilities for location independent working and company servers are now running on cloud servers rather than inside factory premises. Working remotely with mobile phone or laptop is now possible and convenient, and flexible data sharing across supply chain enables new possibilities for SMEs production [19]. Remote working, cloud services and data sharing across supply chain requires access to company network from any location. Remote connectivity sets new challenges for CS, instead of yesterday's complete restriction selective access is required today. IT-management is forced to find a balance between security and flexibility, as firewalls and intrusion detection systems need a complicated set of rules in order to allow authorized access and to block unauthorized access. AI based intrusion detection systems are utilized for dynamic and effective network monitoring [19]. Honeypots are one CS solution for intrusion detection and can be set up to mimic any industrial control device such as PLC, robot controller or IoT-device, working as a decoy to draw the attention of an hacker [2], [20]. Eventually, after logging enough information about his activity and identity, a hacker could be revealed. Most honeypots have been implemented virtual or physical physical [2]. A Virtual honeypot is software running on the cloud or on a local server. A Physical honeypot is a physical device, such as a PLC dedicated for this purpose [20]. Lately also hybrid honeypots have been implemented to combine the best qualities of physical and virtual honeypots [20].

III. Cyber security in manufacturing

When looking for a method for analysing and securing a manufacturing system, protocols and standards provide basic guidelines for security, and vulnerability assessment determines current CS level of the system.

A. Protocols and standards

Development of manufacturing applications and the integration of CPS requires conforming to standards on safety requirements, as set by the Machinery Directive 2006/42/EC. ISO 13849, specifies general principles for design and validation, including a risk assessment executed by the manufacturer of the machinery. Functional safety of electrical, electronic, and programmable electronic control systems are covered by industrial standards IEC 62061. Both standards are inspired by IEC 61508 that addresses the functional safety of electrical, electronic, and programmable electronic safety-related systems. In addition, and most relevant to this work, IT security for networks and systems, is defined by IEC-62443 a standard for industrial communication networks. While seemingly separated, all safety related concerns affect one another, as a CPS operates as a single entity. ISO/IEC 27002 describes good practices and recommendations about information security. This standard was utilized by French National Cybersecurity Agency ANSSI for establishing good CE practices checklist [2]. ISO/IEC27002 does not cover cloud service CS. Good practices for cloud service providers and users are defined in ISO/IEC27017. According to [2] Microsoft Azure, Google Cloud Platform and Amazon Web Services follow ISO/IEC27002 and ISO/IEC27017 standards.

Architecture is the foundation of all functionalities the system can provide. Therefore, security should be initiated from the base of the system. Secure Architecture for Industrial Control Systems (SANS) is a reference architecture for industrial control systems focusing on access control, log management, network security and remote access. It proposes an architecture for the infrastructure of an industrial control system [21]. Other examples of how to secure an industrial control system are NIST 800-82, which covers systems containing distributed control systems (DCS), supervisory control and data acquisition (SCADA) and systems with PLCs and related programmable logic controllers. The NIST standard is utilized in discrete manufacturing, for example automotive and aerospace manufacturing industries [1]. NISTIR 8183, cyber security framework (CSF) [22] describes how to improve CS of existing manufacturing system. Concentrating on the following five functionality areas: Identify, Protect, Detect, Respond, and Recover. Aiming to improve overall CS aspects [22].

B. Vulnerability assessments

Vulnerability assessment of a CPS aims to identify security weaknesses and quantify their impact. Providing knowledge of exactly what should be secure, and why, before specific solutions are selected. The CS market has plenty of tools offering solutions for CS issues, developed by research labs, governmental institutions or by private CS companies. OCTAVE [23], [24] is one of well known approach, aiming to align CS activities with the goals and targets of the organization. Moreover NIST CS Framework was developed to assist industries with securing their infrastructure, to be more resilient to cyber attacks [25]. NIST framework

provides guidance on how to improve CS for existing manufacturing systems. In recent work, NIST framework has been utilized as a SME CS evaluation tool (CET). Framework provides a 35-question online survey for IT-management to self-evaluate company CS maturity within the five NIST framework categories: identify, protect, detect, respond, and recover [10].

IV. Use case demonstrations

As set out by the Digital Europe Programme, Digital Innovation Hubs (DIH) will have an important role to stimulate the uptake of Artificial Intelligence (AI), High Performance Computing (HPC) and CS, for industry and public sector organisations in Europe. TRINITY[1] is one such DIH and has developed a wide set of demonstrators that aim to provide SMEs methods and tools to achieve agile production. Following, these demonstrators are presented and analysed with respect to CS. And if found vulnerable, several CS measures are recommended to be taken.

A. TRINITY core demonstration

Table I lists 18 demonstrators in different areas of robotics and industrial IoT, which were identified as the most promising to advance agile production, but has not yet been widely applied in industrial applications [26]. The specific technologies used in each demonstrator are high-lighted by keywords and, additionally, the technology readiness level (TRL) is presented.

Sixteen out of eighteen Trinity demonstrators focus on robotic functionalities or on systems that support robot programming or interaction. Only two demonstrators do not include robotics, and are focused on IoT. Only one of IoT demonstrators has CS as core functionality. In addition, the technological maturity of the demonstrators has an influence on their CS as well. That is, for technology validated in a lab (TRL4), validated in an industrially relevant environment (TRL5) or demonstrated in an industrially relevant environment (TRL6), the main focus is on functionality and not on the safe integration in operational environments.

B. CS analysis

Table II lists seven CS questions that quickly assess the state of the demonstrators with respect to CS. The questions can be broadly summarized to address three key issues:

KI-1: Cyber secure design - Prior to the design and development of the demonstrator, CS issues were identified and taken into account (Q1, Q3)

KI-2: Cyber security analysis - CS issues were taken into account and documented after development (Q2, Q3)

KI-3: System vulnerability - The technology utilized in the demonstrator can directly explain CS issues (Q4-Q7)

Key issues KI-1 and KI-2 address the greatest concern in current robotics (research) development. With functionality of the technology as main importance, integration typically takes a secondary role, and CS issues are not taken into account during the design stages. This can be clearly identified from the demonstrators as none of the use cases have performed CS analysis to identify potential risks and vulnerability threats during design or prior to the development. In addition, a relatively low number of demonstrators have taken into account and documented CS issues (4 demonstrators, or 24%), and only half of the demonstrators include awareness of CS concerns (9 demonstrators, or 53%).

The final key issue, KI-3, in CS for agile production addressed the particular technology utilized, providing an indication to the state of CS of the demonstrator. Control and operation of the robotic system is divided in three categories, vendor specific controllers (Q4), Programmable Logic Controllers (PLC, Q5) and other industrial communication or middleware systems (Q6). This provides insight into the system architecture and how the data flows. This can also show the vulnerabilities, as in the case of middleware (e.g. ROS1), CS issues are typically not taken into account. The OPC UA standard (IEC 62541) [28] is often used as a middleware to connect industrial equipment together, which has some security features embedded, however, there are still CS flaws/issues in the standard [29].

Vendor specific controllers (7 demonstrators, or 35%) are usually designed with some CS measures. The challenge of these controllers is keeping them up to date and getting updates from the vendors. Keeping vendor specific controllers up to date can be challenging since an industrial robot controller's lifetime is often longer than a standard industrial control system. Unfortunately, this means that some controllers have unpatched vulnerabilities that will never get updated, which is a significant CS risk. In some manufacturing systems having the industrial robot operational all the time is crucial. Therefore, some customers of controllers may postpone updates to the controller [30].

Programmable logic controllers (PLC) are, in simple terms, digital computers for automating an industrial control system [31]. In some systems they are used to control robots or a part of the robotic system. PLCs are placed between the field devices and the human-machine interfaces (HMIs), sending commands and receiving data. PLCs are programmable and can therefore be compromised, by a malicious control program loaded on the controller. It has also been shown that intercepting the communication of a PLC can be compromised with simple python scripts and open-source tolls [32]. However, only 2 demonstrators (12%) use a PLC for control of the system.

Another CS question addresses whether the demonstrator has a web interface, or can be accessed via other means (e.g. intranet, mobile, or cloud). The number of demonstrators that provide this is relatively low (6 demonstrators, or 35%). This might seem good since disconnecting a system from the network limits CS risks. However, a typical cyber physical production system has communication technology, intelligent network and data transmission features [33]. Using intranet, mobile, or the cloud in a manufacturing system could provide more flexibility and agility. Therefore, these systems will eventually need to be updated and connected to a network. This level of connectivity will mandate applying the CS measures regarding a system including a web interface or

TABLE I: Agile production use cases from [27]. Keywords: **HRC** - Human-robot collaboration, **AR** - Augmented reality, **VR** - Virtual reality, **CR** - Collaborative robot, **IR** - Industrial robot, **MR** - Mobile robot, **DT** - Digital twin, **OS** - Operator safety, **IoT** - Internet of Things, **S** - Simulation, **RP** - Robot programming, **CS** - Cyber security. A detailed description of all use cases can be found on `https://trinityrobotics.eu/catalogue/`.

Demonstrators		**Keywords**	**TRL**
1	Collaborative assembly with vision-based safety system	CR, HRC, OS, AR	6
2	Collaborative disassembly with augmented reality interaction	IR, HRC, OS, AR	6
3	Collaborative robotics in large scale assembly, material handling and processing	IR, CR, OS	6
4	Integrating digital context to a digital twin with AR/VR for robotized production	IR, VR, AR, DT	6
5	Wire arc additive manufacturing with industrial robots	IR, IoT	6
6	Production flow simulation/supervision	S, IoT, DT, VR, RP	6
7	Robot workcell reconfiguration	CR, RP, DT	6
8	Efficient programming of robot tasks by human demonstration	CR, HRC, RP	6
9	Dynamic task planning & work re-organization	MR, HRC, RP	5-6
10	HRI framework for operator support in human robot collaborative operations	IR, HRC, AR, OS	5-6
11	Robotized serving of automated warehouse	MR, RP	5
12	User-friendly human-robot collaborative tasks programming	CR, HRC, RP	5
13	Deployment of mobile robots in collaborative work cell for assembly of product variants	CR, MR, RP	5
14	Virtualization of a robot cell with a real controller	S, DT, RP	6
15	IIoT Robustness Simulation	IoT, S, CS	4
16	Flexible automation for agile production	IR, RP	4
17	AI-based stereo vision system for object detection, recognition, classification and pick-up by a robotic arm	CR, RP	4
18	Rapid development, testing and validation of large scale wireless sensor networks for production environment	IoT	4

TABLE II: High-level analysis of the demonstrators to assess and raise awareness of CS. Abbreviations: **DDS** - Data Distribution Service, **OPC** - Open Platform Communications, **OPC-UA** - OPC Unified Architecture.

Cyber security questions		**Applicable use cases**	**Total nr of use cases**	**%**
Q1	A CS analysis defining potential risks and vulnerability threats has been done and documented during design or prior to the development of the use case	none	0	0
Q2	CS concerns have been taken into account and have been documented	3, 4, 14, 15	4	24
Q3	Robotic system developers and engineers are aware of CS concerns in the use case	3, 4, 6, 7, 11-14, 17	9	53
Q4	Robotic systems are designed and operated only by vendor specific controllers	1, 2, 10, 11, 16, 13, 14	7	35
Q5	Robotic systems have been programmed, created and operated by PLCs	10, 14	2	12
Q6	Robotic systems have been programmed and/or are controlled and operated by ROS (1-2), DDS, OPC, OPC-UA, or other available interfaces	1-4, 6, 7, 9, 12, 13, 17	10	59
Q7	Robotic systems have a web interface, can be accessed via intranet, mobiles, internet or can be operated via the cloud	6, 7, 8, 11, 12, 14	6	35

accessed via other mediums.

C. CS measures

Awareness of CS issues have been raised to each individual demonstrator, based on the answers of the CS questions and its analysis. Different measures to harden the systems are then given, as listed in Table III. These are detailed as follows.

Isolation/segmentation or taking the robotic system offline is essential according to many standards, especially SANS [21]. 11 of the demonstrators have either segmented their network or taken it offline. In the case of the demonstrators that have not considered the measurements the components with the different functionality should be segmented from each other. In the case of demonstrator 5 and 6 which is heavily IoT dependent the industrial zone and manufacturing zone should be segmented.

There is only one demonstrator that has considered measurements for white listing of a robotic system. Whitelisting limits the access to the robotic system through limiting work stations and ports at the network level.

Access controlling can be achieved with a AAA-server (authentication, authorization, and accounting) [34]. There are many alternatives for such security capability, but for SMEs open-source choices could better suit the need. Almost all demonstrators have introduced these measures (15 demonstrators or 88%), thereby improving the system's CS and limiting the access to the system.

Vulnerability assessment provides a better prospective of the systems. The business owners can easily identify the existing weaknesses of the system. For two demonstrators (demonstrator 3 and 4), a vulnerability assessment of the robotic system has taken place and all vulnerabilities have been reported and are being handled (M4). The vulnerability assessment can be preformed with open source software such ass NESSUS [35].

CS is not an "add-on" to the network and security should be considered when designing and building a robotics system. The inclusion of security by design principles (M5) has not been taking into account by any demonstrator. The demonstrators are developed by research organisations or universities focusing mainly on robotics, therefore CS has not been considered when designing and building the system and it is an afterthought. Because of this, implementing CS would require major efforts to the re-design and re-implementation of the developed technology. Each of the

TABLE III: Measures to address the CS issues.

Cyber security measures taken		Applicable use cases	Total nr of use cases	%
M1	Isolation: the robotic system has been taken offline, or has been implemented on a segregated network	1, 3, 4, 7, 10-14, 16, 17	11	65
M2	White listing: the robotic system has been integrated in the network, but can only be accessed by a specific set of network operations and other machines	14	1	6
M3	Access, identity & authentication management: access to the robotic system (development and operation) has been limited to a specific set of users/applications, granted upon authentication	1-4, 6-14, 16, 17	15	88
M4	A vulnerability assessment of the robotic system has taken place and all vulnerabilities have been reported and are being handled	3, 4	2	12
M5	The application logic of the robotic system has been developed on the basis of security by design principles, taking into account application security	none	0	0
M6	Security capabilities offered by ROS2 have been considered or have been implemented in the robotic system	3, 4, 7, 12, 17	5	29
M7	Awareness of cyber security issues have been raised, but no serious preventative measures have been taken yet	3, 4, 6, 9-11, 13-15, 17	10	59

demonstrators should re-design the robotic system based on their use case and CS needs. The NIST framework [22] can be applied as approach for such purpose.

ROS2 as middleware has improved CS vulnerabilities, as compared to ROS1, by incorporating authentication, encryption and public key infrastructure. In addition, ROS2 is built upon the Data Distribution Service (DDS) standard. Demonstrators built with ROS1 could therefore migrate to ROS2, or at least consider to do so. This was done by 5 demonstrators or 29%.

A lot of businesses don't take security seriously before any incident. Most of the demonstrators (10 demonstrators, or 59%) are aware of CS issues for the systems, but have not taken any action regarding these issues. This excludes measures such as isolation and basic access control, since these are only minor fixes and do not resolve the CS issues that have been raised. Having awareness of CS issues can prevent further problems.

V. CS RECOMMENDATIONS FOR SMES

The most important CS recommendation for SMEs is to increase their level on CS awareness. Second step should be vulnerability assessment in order to find out existing CS vulnerabilities. Dedicated efforts should then be set to address and tackle current CS issues, and to monitor potential CS issues continuously. As CS may not be part of their core expertise, SMEs should follow these recommendations:

Support - Initiatives to get SMEs cyber secure are plentiful, and actions on (inter)national level should be taken [36].

Education and training - All personnel should be aware of CS issues and receive continuous training on identifying CS risks.

Continuous assessment - Vulnerability assessment should be carried out at regular intervals and documented and reviewed.

In order to secure a system, a number of standards and guidelines such as NIST 800-82 [1] and NIST Framework [22] are available. Following guidelines provided SMEs can implement their systems on a secure base or harden security of their existing systems. It should be noted that standards provide only guidelines and principles for CS, details and implementation is the responsibility of the implementer.

A number of security architectures as foundation for a system has been offered by distinct materials, such as SANS [21]. An architecture provides a base for the functionalities that SMEs implement. Therefore, it is vital to consider a secure architecture for any SME as primary steps. Architectures define computer networking concepts and security implementations such as firewalls and intrusion detection systems. Mentioned implementations are offered as commercial and open source products. Commercial products are often easy for SMEs to utilize but initial cost is out of range. Open source products on the other hand offer a free solution but might require expertise to setup.

CS is a continuous effort and has to be taken seriously, in order to not comprise a SMEs personnel safety, business and environment.

VI. DISCUSSION

The current outlook for novel research and developments in agile production is promising. Multiple standards and protocols exist and can be followed and used as guideline for CS development. Initiatives that support CS are plentiful and national or European wide programs are available for financial (e.g., DIHs) and legislative support [36]. On a practical level, native support for CS and cloud-native applications are becoming the standard as well. This can be identified from product offering of commercial products such as PLCs with native cloud support and open source architectures such as ROS2 with CS as core feature.

However, CS issues can still be found while existing production systems are developed towards Industry 4.0 (e.g., cloud connectivity). For SMEs, the efforts and resources needed for the transitioning can not always easily be found or the skills required need to be obtained elsewhere.

The analyzed demonstrators represent a current offering of the TRINITY use cases and modules for SMEs to adopt, to achieve more agile production. In an ideal situation, CS would have been considered at the design phase of the TRINITY use cases and modules. Unfortunately in almost half of the demonstrators, CS has not been addressed sufficiently and efforts towards hardening require at least partial redesign of the implementation. The reason for this is that most works

are a direct output from research that has only focused on the functional aspects of the demonstrator. However, as this project continues, emphasis is being put on CS and the migration to secure solutions.

VII. Conclusions

CS issues in manufacturing environments can threaten factory operations, lead to data theft and even harm CPS. Especially SMEs are at risk due to a potential lack of resources and knowledge to take dedicated CS measures. In this work we have addressed the state of CS in agile production and have analyzed 18 use case demonstrations, representing technologies and applications towards Industry 4.0. The analysis is done via two tables, one evaluating the functionality of the demonstrators and the other assessing the taken CS measures. An initial CS assessment revealed weak awareness of CS issues within the demonstrators, mainly because the functionality of the systems takes priority over CS. Several measures are presented to harden and secure the demonstrators towards outside attacks. Finally, the most important measure for SMEs to take is to increase awareness of CS related issues, as it is key to SMEs CS hardening.

ACKNOWLEDGMENT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 825196.

References

[1] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security - supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC)," National Institute of Standards and Technology, Tech. Rep., 2011-06-07 2011.

[2] V. Mullet, P. Sondi, and E. Ramat, "A review of cybersecurity guidelines for manufacturing factories in Industry 4.0," *IEEE Access*, vol. 9, pp. 23 235–23 263, 2021.

[3] Q. Zhu and Z. Xu, *Future Work in Security Design of CPSs*. Cham: Springer International Publishing, 2020, pp. 179–183.

[4] A. Kusiak, "Smart manufacturing must embrace big data," *Nature*, vol. 544, no. 7648, pp. 23–25, 2017.

[5] P. Wellener *et al.*, "Deloitte and mapi smart factory study: capturing value through the digital journey," *Deloitte Insights and MAPI, Deloitte, USA*, 2019.

[6] M. Kiss, G. Breda, and L. Muha, "Information security aspects of industry 4.0," *Procedia Manufacturing*, vol. 32, pp. 848–855, 2019, 12th International Conference Interdisciplinarity in Engineering, INTER-ENG 2018, 4–5 October 2018, Tirgu Mures, Romania.

[7] M. Button, "Editorial: economic and industrial espionage," *Security Journal*, vol. 33, pp. 1–5, 2020.

[8] T. Macaulay and B. L. Singer, *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2011.

[9] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, pp. 65–88, 2015.

[10] M. Benz and D. Chatterjee, "Calculated risk? a cybersecurity evaluation tool for SMEs," *Business Horizons*, vol. 63, no. 4, pp. 531–540, 2020.

[11] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *Journal of Manufacturing Systems*, vol. 47, pp. 93–106, 2018.

[12] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, pp. 1–44, 2021.

[13] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability engineering & system safety*, vol. 139, pp. 156–178, 2015.

[14] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, "Current cyber-defense trends in industrial control systems," *Computers & Security*, vol. 87, p. 101561, 2019.

[15] D. Wu, A. Ren, W. Zhang, F. Fan, P. Liu, X. Fu, and J. Terpenny, "Cybersecurity for digital manufacturing," *Journal of manufacturing systems*, vol. 48, pp. 3–12, 2018.

[16] L. A. Kirschgens, I. Z. Ugarte, E. G. Uriarte, A. M. Rosas, and V. M. Vilches, "Robot hazards: from safety to security," *arXiv preprint arXiv:1806.06681*, 2018.

[17] F. Jahan, W. Sun, Q. Niyaz, and M. Alam, "Security modeling of autonomous systems: A survey," *ACM Computing Surveys (CSUR)*, vol. 52, no. 5, pp. 1–34, 2019.

[18] J. Miller, A. B. Williams, and D. Perouli, "A case study on the cybersecurity of social robots," in *ACM/IEEE International Conference on Human-Robot Interaction*, 2018, pp. 195–196.

[19] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, "Addressing industry 4.0 cybersecurity challenges," *IEEE Engineering Management Review*, vol. 47, no. 3, pp. 79–86, 2019.

[20] J. You, S. Lv, Y. Sun, H. Wen, and L. Sun, "Honeyvp: A cost-effective hybrid honeypot architecture for industrial control systems," in *IEEE International Conference on Communications*, 2021, pp. 1–6.

[21] L. Obregon, "Secure architecture for industrial control systems," *SANS Institute InfoSec Reading Room*, 2015.

[22] K. Stouffer, T. Zimmerman, C. Tang, J. Lubell, J. Cichonski, M. Pease, and J. McCarthy, "Cybersecurity framework version 1.1 manufacturing profile," National Institute of Standards and Technology, Tech. Rep., Oct. 2020. [Online]. Available: https://doi.org/10.6028/nist.ir.8183r1

[23] C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson, "Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, version 1.0," Carnegie-Mellon University of Pittsburgh PA Software Engineering Institute, Tech. Rep., 1999.

[24] C. J. Alberts and A. J. Dorofee, *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional, 2003.

[25] M. P. Barrett, "Framework for improving critical infrastructure cybersecurity," *National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep*, 2018.

[26] M. Lanz, J. Reimann, A. Ude, N. Kousi, R. Pieters, M. Dianatfar, and S. Makris, "Digital innovation hubs for robotics – TRINITY approach for distributing knowledge via modular use case demonstrations," *Procedia CIRP*, vol. 97, pp. 45–50, 2021.

[27] ——, "Digital innovation hubs for robotics – trinity approach for distributing knowledge via modular use case demonstrations," *Procedia CIRP*, vol. 97, pp. 45–50, 2021, 8th CIRP Conference of Assembly Technology and Systems.

[28] O. Foundation. OPC unified architecture interoperability for industrie 4.0 and the internet of things. [Online]. Available: https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN.pdf

[29] A. Erba, A. Müller, and N. O. Tippenhauer, "Practical pitfalls for security in OPC UA," 2021.

[30] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero, "An experimental security analysis of an industrial robot controller," in *IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 268–286.

[31] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016.

[32] A. Ghaleb, S. Zhioua, and A. Almulhem, "On PLC network security," *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 62–69, 2018.

[33] J. Wan, B. Chen, M. Imran, F. Tao, D. Li, C. Liu, and S. Ahmad, "Toward dynamic resources management for IoT-based manufacturing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 52–59, 2018.

[34] M. Souppaya and K. Scarfone, "Draft nist special publication 800-46," *Computer*, vol. 33, p. 34.

[35] The nessus family. [Online]. Available: https://www.tenable.com/products/nessus

[36] OECD, *The Digital Transformation of SMEs*. OECD Publishing, 2021. [Online]. Available: https://www.oecd-ilibrary.org/content/publication/bdb9256a-en